



CVE-2023-22912

Published on: Not Yet Published

Last Modified on: 01/26/2023 07:00:00 PM UTC

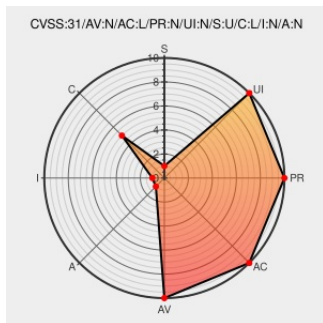
CVE-2023-22912

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Mediawiki](#) from [Mediawiki](#) contain the following vulnerability:

An issue was discovered in MediaWiki before 1.35.9, 1.36.x through 1.38.x before 1.38.5, and 1.39.x before 1.39.1. CheckUser TokenManager insecurely uses AES-CTR encryption with a repeated (aka re-used) nonce, allowing an adversary to decrypt.

CVE-2023-22912 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.3 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	LOW	NONE	NONE

CVE References

Description	Tags	Link
⚓ T315123 CVE-2023-22912: CheckUser TokenManager insecurely uses AES-CTR encryption with repeated nonce, allowing an adversary to decrypt	phabricator.wikimedia.org text/html	MISC phabricator.wikimedia.org/T315123

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
------	--------	---------	---------	--------	---------	----------

Application	Mediawiki	Mediawiki	All	All	All	All
Application	Mediawiki	Mediawiki	1.39.0	-	All	All
Application	Mediawiki	Mediawiki	1.39.0	rc0	All	All
Application	Mediawiki	Mediawiki	1.39.0	rc1	All	All
cpe:2.3:a:mediawiki:mediawiki:*:*:*:*:*:						
cpe:2.3:a:mediawiki:mediawiki:1.39.0:-:*:*:*:*:						
cpe:2.3:a:mediawiki:mediawiki:1.39.0:rc0:*:*:*:*:						
cpe:2.3:a:mediawiki:mediawiki:1.39.0:rc1:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
🔒 @CVEreport	CVE-2023-22912 : An issue was discovered in MediaWiki before 1.35.9, 1.36.x through 1.38.x before 1.38.5, and 1.39.... twitter.com/i/web/status/1...	2023-01-20 18:07:14
🔒 @threatmeter	CVE-2023-22912 MediaWiki up to 1.35.8/1.38.4/1.39.0 nonce re-use A vulnerability classified as problematic was fo... twitter.com/i/web/status/1...	2023-01-21 01:50:34

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report